VL E-GOVERNANCE & IT SOLUTIONS LIMITED

RISK MANAGEMENT POLICY

Risk management is attempting to identify and then manage threats that could severely impact or bring down the organization. Generally, this involves reviewing operations of the organization, identifying potential threats to the organization and the likelihood of their occurrence, and then taking appropriate actions to address the most likely threats.

The Companies Act, 2013 and the SEBI Listing Obligations and Disclosure Requirements) Regulations, 2015, ("LODR - 2015") have also incorporated various provisions in relation to Risk Management policy, procedure and practices.

As per Regulation 17(9) of the SEBI LODR, 2015, the listed entity shall (a)lay down procedures to inform members of board of directors about risk assessment and minimization procedures. (b) The board of directors shall be responsible for framing, implementing and monitoring the risk management plan for the listed entity.

Section 134(3)(n) of the Companies Act, 2013 requires a statement to be included in the report of the board of directors ("Board") of VL E-GOVERNANCE & IT SOLUTIONS LIMITED (the "Company"), indicating development and implementation of a risk management policy for the Company, including identification therein of elements of risk, if any, which, in the opinion of the Board, may threaten the existence of the Company.

Further, the provisions of Section 177(4)(vii) of the Companies Act, 2013 require that every Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall inter alia include evaluation of risk management systems.

In line with the above requirements, it is therefore, required for the Company to frame and adopt a “Risk Management Policy” (“Policy”) of the Company.

VL E-Governance & IT Solutions Limited, being a listed company, is required to adhere to the regulations made both by the Companies Act, 2013 and LODR - 2015 governed by the Securities and Exchange Board of India (SEBI). Where any stipulation is common between the regulations, more stringent of the two shall be complied with.

1. Introduction

The Board of Directors of VL E-Governance & IT Solutions Limited has adopted the following policy and procedures with regard to risk management as defined below. The Board may review and amend this policy from time to time.

2. Definitions

"Audit Committee" means Committee of Board of Directors of the Company constituted under the provisions of the Companies Act, 2013 and SEBI LODR, 2015.

"**Board of Directors**" or “**Board**” in relation to a Company, means the collective body of Directors of the Company.

"**Policy**" means Risk Management Policy.

3. Back Ground And Implementation

The Company is prone to inherent business risks. This document is intended to formalize a risk management policy, the objective of which shall be identification, evaluation, monitoring and minimization of identifiable risks.

This policy is in compliance with the amended LODR - 2015 which requires the Company to lay down procedure for risk assessment and procedure for risk minimization.

The Board of Directors of the Company and the Audit Committee shall periodically review and evaluate the risk management system of the Company so that the management controls the risks through properly defined network.

Head of Departments shall be responsible for implementation of the risk management system as may be applicable to their respective areas of functioning and report to the Board and Audit Committee.

4. Objective

This policy is framed to set up a framework for risk assessment and minimization procedures. The main objective of this policy is to ensure sustainable business growth with stability and to promote a pro-active approach in reporting, evaluating and resolving risks associated with the business. In order to achieve the key objective, the policy establishes a structured and disciplined approach to Risk Management, in order to guide decisions on risk related issues.

5. The specific objectives of the Risk Management Policy are:

1. To ensure that all the current and future material risk exposures of the company are identified, assessed, quantified, appropriately mitigated, minimized and managed i.e to ensure adequate systems for risk management.

2. To establish a framework for the company's risk management process and to ensure its implementation.

3. To enable compliance with appropriate regulations, wherever applicable, through the adoption of best practices.

4. To assure business growth with financial stability.

6. KEY DEFINITIONS:

- Risk Assessment – The systematic process of identifying and analysing risks. Risk Assessment consists of a detailed study of threats and vulnerability and resultant exposure to various risks.

- Risk Management – The systematic way of protecting business resources and income against losses so that the objectives of the Company can be achieved without unnecessary interruption.

- Risk Management Process - The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

7. Risk Management and Risk Monitoring

In principle, risk always result as consequences of activities or as a consequence of non-activities. Risk Management and Risk Monitoring are important in recognizing and controlling risks. The below paragraphs embraces Company's risk identification and mitigation strategies like risk control, avoidance, etc.

Operational Risks:

➢ Swiftness in Government Policies:

The Company's business is dependent on Government policy towards financial inclusion stand and the speed of implementation. Thus, any change in the policy framework and restrictions on the transaction may affect the profitability of business.
Mitigation: Risks that are likely to emanate are managed by constant engagement with the Government, reviewing and monitoring the country's economical and financial related policies and involvement in representative industry-bodies.

➢ Rapid Changes in Technology/Obsolescence of Technology:

Rapid technological changes may change all the existing business models. The Company's margins may hit due to new cost effective disruptive innovations.

Mitigation: The Company strongly believes that technological obsolescence is a practical reality. Technological obsolescence is evaluated on a continual basis and the necessary investments are made to bring in the best of the prevailing technology.

➢ Legal Risk:

Legal risk is the risk in which the Company is exposed to legal action. As the Company is governed by various laws and the Company has to do its business within four walls of law, the Company is exposed to legal risk.

Mitigation: As the Company is governed by various laws and the Company has to do its business within four walls of law, where the Company is exposed to legal risk exposure. We have an experienced team of professionals, advisors who focus on evaluating the risks involved in a contract, ascertaining our responsibilities under the applicable law of the contract, restricting our liabilities under the contract, and covering the risks involved so that they can ensure adherence to all contractual commitments.

➢ Financial Reporting Risks

Changing laws, regulations and standards relating to accounting, corporate governance and public disclosure, Securities and Exchange Board of India (SEBI) rules, and Indian stock market listing regulations are creating uncertainty for companies. These new or changed laws, regulations and standards may lack specificity and are subject to varying interpretations. Their application in practice may evolve over time, as new guidance is provided by regulatory and governing bodies. This could result in continuing uncertainty regarding compliance matters and higher costs of compliance as a result of ongoing revisions to such corporate governance standards.

Mitigation: The Company is committed on maintaining high standards of corporate governance and public disclosure and our efforts to comply with evolving laws, regulations and standards in this regard would further help us address these issues.

➢ Risk of Corporate accounting fraud:

Accounting fraud or corporate accounting fraud are business scandals arising out of Misusing or misdirecting of funds, overstating revenues, understating expenses etc.

The Company mitigates this risk by:

- Understanding the applicable laws and regulations
- Conducting risk assessments,
- Enforcing and monitoring code of conduct for key executives
- Instituting Whistleblower mechanisms
- Deploying a strategy and process for implementing the new controls
- Adhering to internal control practices that prevent collusion and concentration of authority
- Employing mechanisms for multiple authorization of key transactions with cross checks
- Scrutinizing of management information data to pinpoint dissimilarity of comparative figures and ratios
- Creating a favorable atmosphere for internal auditors in reporting and highlighting any instances of even minor non-adherence to procedures and manuals and a host of other steps throughout the organization.

➢ Cyber attack and data leakage:

Increasing concern for user data privacy, data leakage, and number of cyber-attacks are the reason for rising attention to the question of data security, which became more relevant in the recent years. The increasing number of devices connected to the internet not only creates more data but also makes it more vulnerable and not very well protected. It is expected that security analytics costs will raise up. Thus, it is critical to keep up with latest trends in the field of data security.

Mitigation: Privacy and security of data are two of our biggest concerns. However, we have been continuously working in the direction of protecting data. We have adopted below approaches for data security and privacy:

Validation and filtration of end-point inputs: we use an authentic and legitimate end-point device. End-point devices are the entry point for authentic and valid data into the system.
Mandatory Access Control (MAC): in which the access of each user is constrained to a very limited set of tasks and time frame.
Digital signatures using asymmetric encryption: regular audits, and hash chaining are standard practices followed to secure the data.
Monitor logs on a real-time basis to spot anomalies that identify any misuses and abnormality.
Use data tagging and enforced time stamps to help in tracing unauthorized activity.
Encryption at all times – when data is in transit and at rest, database contents is encrypted; protecting data at rest, and additional protection for data in transit applied using SSL encryption to connect the client and server, ensuring that only trusted computers can access the encrypted data. Encryption is a crucial part of maintaining confidentiality and integrity of data.
Encryption of data within the database, access control, masking sensitive data and stringent authorization policies, keeping security patches up to date. Deploying encryption on all data on a granular basis helps ensure that even if there is a system breach, the data itself remains protected.
Granular auditing: We analyse various kinds of logs which is always advantageous and helpful in recognising any kind of cyber-attack or malicious activity.
Data Provenance: We classify data, as it is necessary to be aware of its origin to determine the data origin accurately, authentication, validation and access control could be gained.

Constitution of Risk Management Committee

The Company has constituted a Risk Management Committee with majority of Members of the Board of Directors, with the overall responsibility of overseeing and reviewing risk management across the Company. The terms of reference of the Risk Management Committee are as follows:

- review of strategic risks arising out of adverse business decisions and lack of responsiveness to changes;
- review of operational risks;
- review of financial and reporting risks;
- review of compliance risks;
- review or discuss the Company's risk philosophy and the quantum of risk, on a broad level that the Company, as an organization, is willing to accept in pursuit of stakeholder value;
- review the extent to which management has established effective enterprise risk management at the Company;
- inquiring about existing risk management processes and review the effectiveness of those processes in identifying, assessing and managing the Company's most significant enterprise-wide risk exposures;
- review the Company's portfolio of risk and consider it against it's risk appetite by reviewing integration of strategy and operational initiatives with enterprise-wide risk exposures to ensure risk exposures are consistent with overall appetite for risk; and
- review periodically key risk indicators and management response thereto.

Meetings

The Risk Management Committee shall meet at least twice in a year whenever constituted in the company subject to maximum gap between two meetings shall not be more than 210 day or as amended in the applicable law time to time.

Authority

The Committee shall have free access to management and management information. The Committee, at its sole authority, may seek the advice of outside experts or consultants where judged necessary.

Role of the Board

The Board will undertake the following actions to ensure risk is managed appropriately:

1. The Board shall be responsible for framing, implementing and monitoring the risk management plan for the company.
2. The Board shall ensure that the SOPs of all departments & verticals are prepared as per best global practices and are compliant with ESG parameters are free from any business or legal risks.
3. The Board shall define the roles and responsibilities of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the Committee and such other functions as it may deem fit.
4. Ensure that the appropriate systems for risk management are in place.
5. The independent directors shall help in bringing an independent judgment to bear on the Board's deliberations on issues of risk management and satisfy themselves that the systems of risk management are robust and defensible; Participate in major decisions affecting the organization's risk profile;
6. Have an awareness of and continually monitor the management of strategic risks;
7. Be satisfied that processes and controls are in place for managing less significant risks;
8. Be satisfied that an appropriate accountability framework is working whereby any delegation of risk is documented and performance can be monitored accordingly;
8. Ensure risk management is integrated into board reporting and annual reporting mechanisms;
9. Convene any board-committees that are deemed necessary to ensure risk is adequately managed and resolved where possible.

Review

This policy shall be reviewed at a minimum at least every year to ensure it meets the requirements of legislation & the needs of organization.